*The Columbia*
SCIENCE AND TECHNOLOGY LAW REVIEW
www.stlr.org

# DIGITAL RIGHTS MANAGEMENT: MANY TECHNICAL CONTROLS ON DIGITAL CONTENT DISTRIBUTION CAN CREATE A SURVEILLANCE SOCIETY

By Chris Jay Hoofnagle*

Digital Rights Management technologies threaten to fundamentally alter the level of privacy protection United States law and tradition currently provide to media consumers. If left unchecked, the development and implementation of DRM could lead to a "surveillance" society. This essay proposes eight policy principles to extend privacy protection to the distribution of digital media.

## I. ANONYMOUS CONTENT CONSUMPTION AND DIGITAL RIGHTS MANAGEMENT

In the opening scenes of Patrick McGoohan's *The Prisoner*, a former intelligence agent arrives at a remote paradise prison and tries to use a telephone. The telephone operator asks the agent to identify himself: "What is your number sir?" The agent replies, "I haven't got a number." The operator refuses to connect the call, saying, "No number, no calls!"[1] McGoohan's lesson, which was more fully developed as the series continued, was that a surveillance society would control access to communications and culture through identification. Ubiquitous identification requirements would lead to dossier building and a culture of strong social control. We don't live in such a society, but we could develop a dossier society if copyright control mechanisms are deployed in a manner that is insensitive to privacy.

Today, individuals are free to anonymously explore different ideas presented in books, music, and movies.[2] Bricks and mortar transactions allow individuals to purchase media with cash without leaving any personally identifiable record.[3] Similarly, many

* Chris Jay Hoofnagle is the Associate Director at the Electronic Privacy Information Center, 1718 Connecticut Ave. NW 200, Washington, DC 20009, chris@epic.org.

[1] *The Prisoner: Arrival* (Everyman Films/ITC television broadcast, Sept. 29, 1967).

[2] *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 Conn. L. Rev. 981 (1996).

[3] Even where a customer record is created, many booksellers will resist law enforcement access to customers' personal information. *See e.g.* Associated Press, *Court Overturns Bookstore Ruling*, Wired

libraries have developed circulation systems that retain no transaction record once the borrowed media is returned.[4] In these systems, tracking or reporting on individuals' media consumption habits is difficult. It is laborious, and gives staff members or owners enough time to question whether the transaction information should be conveyed to law enforcement or marketers.

It is unclear whether this level of privacy protection will be carried into the digital content environment. Computer networks allow digital dissemination of almost any media, anytime, to anyone with a broadband connection. With the advent of easy to use peer-to-peer software applications, many Internet users have used this new technology to engage in outright piracy by freely trading copyrighted digital content. In reaction, content owners have proposed Digital Rights Management ("DRM") systems. DRM systems restrict the use of digital files in order to protect the interests of copyright holders. DRM technologies can control file access (number of views, length of views) and prevent or allow in varying degrees the altering, sharing, copying, printing, and saving of the file. These technologies may be contained within the operating system, program software, in the actual hardware of a device, or a combination of all three. It is assumed that through deploying DRM and the architecture needed to support the technologies, piracy will be curbed.

DRM systems take two approaches to securing content. The first is "containment," an approach where the content is encrypted in a shell so that it can only be accessed by authorized users.[5] The second is "marking," the practice of placing a watermark, flag, or an XrML tag on content as a signal to a device that the media is copy protected.[6] Some systems combine the two approaches. Nevertheless, according to Princeton University Computer Science Professor Ed Felten, DRM systems are vulnerable to cracking by individuals with moderate programming skills.[7]

Some existing DRM systems implicate privacy because they allow copyright owners to monitor private consumption of content. In an attempt to secure content, many DRM systems require the user to identify and authenticate a right of access to the protected media. In the case of Microsoft's eBook Reader,[8] this means that the media software and user's choices in electronic books are digitally linked not only to the user's

---

Magazine (Apr. 9, 2002), *available at* http://www.wired.com/news/privacy/0,1848,51667,00.html; Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083 (2002).

[4] *See generally*, Mary Minow, *Library Patron Internet Records and Freedom of Information Laws*, 9 California Libraries 8 (Apr. 4, 1999).

[5] Professor Edward Felten, Address at the Boalt Hall Copyright Workshop (Mar. 22, 2002): E-mail from Edward Felten, Professor of Computer Science, Princeton University, to Chris Hoofnagle, Associate Director, Electronic Privacy Information Center (Feb. 17, 2004, 19:11:32 EST) (on file with author).

[6] *Id.*

[7] *Id.*

[8] eBook Reader is a software program that allows individuals to view electronic books on computers and other devices. *See* Microsoft Reader General Questions, *at* http://www.microsoft.com/reader/info/support/faq/general.asp (last visited Mar. 18, 2004).

computer, but also to Microsoft Passport, the company's identity management system.[9] This arrangement allows tracking of both the individual and the individual's computer. Some systems, such as Microsoft's Windows Media Player, assign a Globally Unique Identifier (GUID) to the media device that facilitates tracking.[10] These systems create records that enable profiling and target marketing of individuals' tastes by the private sector.

A recent lawsuit illustrates how DRM implementations can invade privacy. In February 2002, Sunncomm, Inc., a DRM systems developer, and Music City Records settled a lawsuit by a California woman who objected to their practice of tracking and disclosing personal information—including music consumption patterns—to third-parties with no opt-out scheme. The plaintiff's attorney, Ira Rothken, filed suit under a broad California consumer protection statute, arguing that SunnComm: "never disclose[d] on the shrink-wrap of the CD(s) that consumers cannot listen to music on their computers anonymously. If left unchecked, this will be the start of an era where consumers will be coerced to give up their privacy to listen to music on their computers."[11] The settlement agreement required the companies to provide notice to consumers of their information collection practices and to refrain from requiring consumers to disclose their personal information as a condition of downloading, playing, or listening to a CD.[12] While this settlement agreement is important, not all Americans can avail themselves of California's consumer protection laws. Given adequate notice to consumers, it is likely that other states and the Federal Trade Commission will not object to Sunncomm-style DRM systems and will assume that users consciously and freely accept the invasion of their privacy when buying the product. Users of these new systems will be taken from a culture where there is freedom to enjoy media anonymously to one where access will be conditioned upon revealing one's identity. Once the individual has given up his freedom of anonymity, media companies will claim that they have the freedom to exploit information about the individual's media consumption by selling it to others—perhaps even the government.[13]

---

[9] This service is now called ".Net Passport." *See* Russel Kay, *Copy Protection: Just Say No*, Computerworld, (Sept. 4, 2000); Chris Jay Hoofnagle, *Overview of Consumer Privacy 2002*, 701 Practicing Law Institute 1339 (2002), *available at* http://www.epic.org/epic/staff/hoofnagle/plidraft2002.pdf; Chris Jay Hoofnagle, *Digital Rights Management and Privacy*, Presentation to the Santa Clara University Law School Symposium on Information Insecurity, Feb. 8, 2002, *at* http://www.epic.org/epic/staff/hoofnagle/drm.ppt; Megan E. Gray & Will Thomas DeVries, *The Legal Fallout From Digital Rights Management Technology*, 20 Comp. & Internet Lawyer 20 (April 2003).

[10] Richard Smith, *Serious Privacy Problems in Windows Media Player for Windows XP*, Computerbytesman, Feb. 20, 2002, *at* http://www.computerbytesman.com/privacy/wmp8dvd.htm.

[11] DeLise v. Fahrenheit, No. CV-014297 (Cal. Sup. Ct. Sept. 6, 2001) (Pl. Comp. at ¶ 1), *available at* http://www.techfirm.com/mccomp.pdf.

[12] Press Release, SunnComm, Inc., *Sunncomm and Music City Records Agree to Resolve Consumer Music Cloqueing Law Suit by Providing Better Notice and Enhancing Consumer Privacy* (Feb. 22, 2002), *at* http://www.techfirm.com/sunnsett.pdf.

[13] Solove, *supra* note 3, at 1090.

## II. U.S. LAW AND TRADITION HAS PROTECTED PRIVACY OF MEDIA CONSUMERS

Traditionally, federal and state law has set out standards to protect individuals' choices in consumption of media.[14] It is understood that in this context, privacy protection provides the developmental space needed for individuals to hone skills necessary to exercise First Amendment freedoms. After all, individuals' autonomy cannot be developed unless they have the freedom to explore ideas without overbearing social control. As Professor Julie Cohen has noted:

> Autonomous individuals do not spring full-blown from the womb. We must learn to process information and to draw our own conclusions about the world around us. We must learn to choose, and must learn something before we can choose anything. Here, though, information theory suggests a paradox: "Autonomy" connotes an essential independence of critical faculty and an imperviousness to influence. But to the extent that information shapes behavior, autonomy is radically contingent upon environment and circumstance. The only tenable resolution—if "autonomy" is not to degenerate into the simple, stimulus-response behavior sought by direct marketers—is to underdetermine environment. Autonomy in a contingent world requires a zone of relative insulation from outside scrutiny and interference—a field of operation within which to engage in the conscious construction of self. The solution to the paradox of contingent autonomy, in other words, lies in a second paradox: To exist in fact as well as in theory, autonomy must be nurtured.[15]

Recognizing this need for insulation from outside scrutiny and interference, librarians incorporated formal policies in their code of ethics for protecting patron privacy in 1939.[16] Also, the states have erected a framework of protections for library circulation records.[17] Congress acted to protect television viewing habits by enacting the Cable Communications Policy Act of 1984.[18] Under the act, cable operators must obtain opt-in

---

[14] *See generally* Marc Rotenberg, *The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments* (2002).

[15] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1424 (2000).

[16] Article 11 specifies: "It is the librarian's obligation to treat as confidential any private information obtained through contact with library patrons." 1939 Code of Ethics for Librarians, American Library Association (1939), *available at* http://www.ala.org/Template.cfm?Section=History1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=8875.

[17] Robert Ellis Smith, *Compilation of State and Federal Privacy Laws* 40-41 (Privacy Journal 2002).

[18] Cable Communications Policy Act, 47 U.S.C § 551 et seq. (2003).

consent before transferring user data to third parties.[19] They must also regularly destroy users' data.[20] Similarly, the Video Privacy Protection Act of 1998 was passed by Congress to create opt-in protections for those who rent media on video tape.[21] That act specifies procedures for law enforcement access to customer records[22] and requires regular data destruction.[23] Both laws allow individuals to access their data,[24] and both carry civil remedies for violation.[25]

These protections were developed in recognition that monitoring influences behavior, and that the threat of content monitoring will chill behavior and result in less freedom for individuals. The data collected from content consumption could be used for any number of purposes—from direct marketing to government profiling of political ideals. One could even imagine an employer who would be interested in knowing that their prospective employees read certain books or listen to politically-charged music. An employer sensitive to labor organization, for instance, may want to stay away from fans of Rage Against the Machine in favor of listeners with more pedestrian tastes.

New business models can disrupt these strong privacy protections.[26] For instance, although they serve the same general purpose, bookstores generally are not subject to the ethical obligations and privacy laws that bind libraries. In fact, the privacy policies of Amazon.com and Barnes & Noble.com make it clear that personal may be transferred to affiliates and others.[27] Barnes and Noble even reserves the right to disclose sales records to law enforcement based on the company's "good judgment."[28] Amazon's policy on release of information to law enforcement is not as clear.[29]

New technologies can also disrupt privacy protections. Although cable providers must obtain consent from a subscriber, a "personal video recorder" service provider, such

---

[19] 47 U.S.C. § 551(c).

[20] 47 U.S.C. § 551(e).

[21] Video Privacy Protection Act, 18 U.S.C. § 2710 (2003).

[22] 18 U.S.C. § 2710(b)(3).

[23] 18 U.S.C. § 2710(e).

[24] 47 U.S.C. § 551(d); 18 U.S.C. § 2710(b)(2)(A).

[25] 47 U.S.C. § 551(f); 18 U.S.C. § 2710(c).

[26] For a discussion of the failures of sectoral privacy frameworks, *see* Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 Berkeley Tech. L.J. 283 (2003).

[27] Amazon.com Privacy Notice, *available at* http://www.amazon.com/exec/obidos/tg/browse/-/468496/002-5512475-7444016 (2003); Barnes & Noble.com Privacy Policy, *available at* http://www.barnesandnoble.com/help/nc_privacy_policy.asp (2003).

[28] Law Enforcement Investigations, Privacy Policy, BarnesandNoble.com (2003).

[29] *See* Solove, *supra* note 3.

as Tivo, isn't subject to the Video Privacy Protection Act. Although Tivo can monitor minute-by-minute consumption choices, placing it in a similar position to a cable provider, the Act only applies to cable operators or their affiliates.[30] The advent of DVDs creates a similar issue with regard to the Video Privacy Protection Act. The Act covers companies that rent, sell, or deliver "prerecorded video cassette tapes or similar audio visual materials," but no court has determined whether providers of DVDs are subject to this definition.[31]

## III. SUCCESSFUL DRM TECHNOLOGY WILL PROTECT INDIVIDUALS' PRIVACY

Because DRM is a topic of heightened public interest, the Electronic Privacy Information Center (EPIC) and other not-for-profit civil liberties and consumer protection groups have urged policymakers to shape the technology so that it is sensitive to individuals' privacy.[32] They primarily have argued that collection of personal data should be subject to Fair Information Practices (FIPs), principles that set out the rights and responsibilities of data subjects and data collectors.[33] The most commonly accepted articulation of FIPs was created by the Organization for Economic Coordination and Development (OECD). That articulation takes the form of eight data guidelines, or "principles," for addressing the collection and maintenance of personal information.[34] The OECD specifies that these principles are the minimum standards for the protection of privacy. Policymakers are encouraged to establish protections that go beyond the eight principles to guarantee the privacy and security of personal data. These principles are as follows:

1. The collection limitation principle specifies that information should be collected lawfully and fairly, and with the consent of the data subject. Collection limitation also implies that data collectors should "minimize" their data collection. That is, only the minimum amount of data necessary to process a transaction should be collected. This principle has been overlooked in American e-commerce. In fact, many of the

---

[30] 47 U.S.C. § 551(a)(2)(C).

[31] 18 U.S.C. § 2710(a)(4); *see also* Will Thomas DeVries, *The Video Privacy Protection Act*, EPIC (Aug. 6, 2002), *available at* http://www.epic.org/privacy/vppa/.

[32] EPIC and the Electronic Frontier Foundation have elsewhere argued that DRMs should respect fair use rights, and not impinge upon users' choice to use free or open-source software. *See* Letter from EPIC and the Electronic Frontier Foundation to Chairman Coble, House Judiciary Subcommittee On the Courts, the Internet and Intellectual Property (Jun. 5, 2002), *available at* http://www.epic.org/privacy/drm/hjdrmltr6.5.02.html.

[33] *See generally*, Marc Rotenberg, *What Larry Doesn't Get: Fair Information Practices and the Architecture of Privacy*, 2001 Stan. Tech. L. Rev. 1 (2001).

[34] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Organization for Economic Cooperation and Development (1980), *at* http://www.oecd.org/document/20/0,2340,en_2649_201185_15589524_1_1_1_1,00.html.

profilers in the "Customer Relations Management" industry urge businesses to collect the maximum amount of information from individuals.[35] There are substantial benefits to following a policy of minimization. In many circumstances, when entities collect less information they assume less risk by reducing the amount of information that could be misused by malicious hackers or by employees. Additionally, the privacy policies of entities that minimize information collection tend to be simpler to write and easier for individuals to digest.

In the DRM context, collection limitation would discourage content owners from forcing a consumer to identify himself for the benefit of accessing online entertainment. Instead, a successful system will only confirm the eligibility of a particular consumer to perform certain actions (i.e. receive a subscription, fill a prescription, make a bill payment, etc.).[36]

2. The data quality principle specifies that personal data should be accurate, complete, and up to date. This principle encourages data collectors to engage in regular data destruction, thus protecting users if business models or privacy practices change to the detriment of the consumer.

3. The purpose specification principle requires that data collectors give notice of the purposes for which personal information is collected. This notice should be given when the data is collected.

4. The use limitation principle specifies that data collected for one purpose should not be employed for another purpose absent consent. For example, use limitation is violated by magazine companies that transfer their subscription lists, which are collected for the purpose of mailing a publication, to marketers who use the subscription lists for direct mailings. In the DRM context, it would be inappropriate to use personal information collected in securing content for direct marketing or other purposes.

5. The security safeguards principle requires data collectors to protect personal information from loss, unauthorized access, destruction, improper use, modification, or disclosure.

6. The openness principle requires data collectors to be forthcoming with information about database practices. Policies involving the use and maintenance of the databases should be public, and there should be no secret databases.

---

[35] Harold Zimmerman, Remarks at the Meeting of the Direct Selling Education Foundation on Facets of Customer Relations Management (May 21, 2001). Mr. Zimmerman recommends that incentives be given to sales employees so that they will collect the maximum amount of personal data and input the information into a database.

[36] Pamela Samuelson, Copyright and Censorship, Keynote address at the Censorship & Privacy Conference, Faculty of Law, University of Toronto, (January 25, 2002), *in* Jason Young Conference Notes, January 30, 2002, *at* http://www.lexinformatica.org/dox/censorship.pdf *at* 4.

7. The individual participation principle requires that data subjects have access to and a right to correct their personal information stored in databases.

8. The accountability principle specifies that data collectors should be responsible for complying with FIPs. This responsibility comes in the form of legal liability. Privacy violations should give rise to a private right of action where data collectors can be held responsible for liquidated damages and legal fees.

These eight principles will allow individuals to enjoy new communication systems and a rich array of media. Without these principles, content owners and software designers may create DRM systems that invade individuals' privacy. Indeed, many DRM systems have already been designed without sensitivity to individuals' privacy. To prevent a surveillance society where individuals' access to media and new ideas is conditioned upon revealing identity, it is important for policymakers to follow the precedent of privacy protection for content in the offline world and create new privacy protections for the distribution of digital media.